

Remarks

In the non-final Office Action dated July 15, 2008, the following rejections are presented: claim 3 stands rejected under 35 U.S.C. § 112(2); claims 1-3 stand rejected under 35 U.S.C. § 101; claims 1, 4-5, 9-10 and 12-15 stand rejected under 35 U.S.C. § 102(b) over Satoh (“A Compact Rijndael Hardware Architecture with S-Box Optimization” (c) 2001); claims 2-3, 6-7, 11, and 16-18 stand rejected under 35 U.S.C. § 103(a) over the Satoh reference in view of Applicant’s Admitted Prior Art; claim 8 stands rejected under 35 U.S.C. § 103(a) over the Satoh reference in view of Jarvinen (“A Fully Pipelined Memoryless 17.8 Gbps AES-128 Encryptor”). Claim 4 is objected to due to informalities. The Office Action notes that Applicant has not complied with one or more conditions for receiving the benefit of an earlier filing date under 35 U.S.C. § 119(e). Applicant addresses these rejections in the following discussion which does not acquiesce in any regard to averments in this Office Action (unless Applicant expressly indicates otherwise).

Applicant has amended claim 1 in a manner that renders the rejections of claims 1-3 under 35 U.S.C. § 101 moot. In pertinent part, claim 1 expressly recites that the S-box is a circuit and that the various transformations are implemented using circuitry. Notwithstanding the amendments, Applicant respectfully traverses each of the rejections because the Office Action bases the rejection upon an improper interpretation of the claims. For instance, the Office Action has alleged that “an S-box alone does not constitute performing the SubByte function of the Rijndael Block Cipher.” *Instant Office Action*, page 4, no. 10. Applicant is not certain what hypothetical function the Office Action has in mind, but notes that the claim language does not require functionality other than that which is claimed. In pertinent part, claim 1 recites “a SubByte function,” the particulars of which are defined by the claim. The Office Action appears to read limitations into the claim that relate to a specific and hypothetical SubByte function that is not required by the claims. Contrary to the assertion of the Office Action, the claimed SubByte function does not require that each and every possible function associated with SubBytes of a Rijndael Block Cipher be performed. Instead, the claims require those functions recited. For the aforementioned reasons, Applicant respectfully requests that the rejections be withdrawn.

Applicant respectfully traverses the rejection of claim 3 under 35 U.S.C. § 112(2). Applicant submits that the recited elements are introduced in claim 3 in a manner that further limits elements of claim 1. M.P.E.P. 2173.05 explains that antecedent basis problems might arise in the following cases:

- where a claim refers to "said lever" or "the lever," where the claim contains no earlier recitation or limitation of a lever and where it would be unclear as to what element the limitation was making reference;
- if two different levers are recited earlier in the claim, the recitation of "said lever" in the same or subsequent claim would be unclear where it is uncertain which of the two levers was intended; and
- a claim which refers to "said aluminum lever," but recites only "a lever" earlier in the claim, is indefinite because it is uncertain as to the lever to which reference is made.

None of these examples correspond to the present case (*i.e.*, the elements were not preceded by language such as "said" or "the"). Instead, the identified elements are introduced for the first time in claim 3. Moreover, M.P.E.P. 2173.05 also explains that "the failure to provide explicit antecedent basis for terms does not always render a claim indefinite." Accordingly, claim 3 is not indefinite for lack of antecedent basis and Applicant requests that the rejection be withdrawn.

Applicant respectfully traverses the rejections under 35 U.S.C. § 102(b) for failing to show correspondence to each element as claimed. Applicant notes that the Satoh reference appears to be directed at an implementation that does away with lookup tables. Thus, the Office Action's reliance upon Satoh to teach correspondence to Applicant's claimed invention, which uses lookup tables, is misplaced.

Applicant respectfully submits that the Office Action is improperly relying upon components from two different embodiments, which are clearly distinguished from one another by the teachings of the Satoh reference. Satoh teaches an S-box is improved over look-up table methods. More specifically, a primary purpose of the Satoh reference is to reduce gate count by removing the need for a lookup table. As explained in Satoh, "S-box lookup tables appear as random numbers to CAD tools, and therefore logic compression is very hard." *Satoh*, page 249. Applicant submits that it is therefore improper to assert correspondence under 35 U.S.C. § 102(b) for elements taken from two

different circuits. Moreover, a primary purpose for implementing the combinational logic circuit described in Section 3.1 is to do away with lookup table approach described in connection with Section 2. Thus, the Office Action has improperly interpreted the teachings of the Satoh reference and therefore has not shown the element arranged as claimed. Applicant respectfully requests that the rejections be withdrawn.

Applicant respectfully traverses each of the rejections under 35 U.S.C. § 103(c) for relying upon an improper interpretation and for failing to show correspondence to each element. As discussed in connection with the rejections under 35 U.S.C. § 102(b), the underlying premise for the rejection of each of the independent claims is improper. As each of the rejections under 35 U.S.C. § 103(c) rely upon this same premise and the alleged modification does not cure the impropriety, the rejections under 35 U.S.C. § 103(c) are also improper.

Moreover, Applicant notes that the Office Action fails to properly address the limitations of various dependent claims. For instance, claim 3 includes limitations directed towards a specific combinational logic circuit. The Office Action, however, fails to show correspondence to this combinational logic circuit. Applicant challenges the Office Action's assertion that Fig. 1 of Satoh corresponds to the claim limitations. Applicant has reproduced the relevant portion of the cited Fig. 1 of Satoh. Applicant notes that this aspect does not teach or suggest correspondence to the claim limitations.

$$b_{ij} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} a_{ij}^{-1} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

- Satoh, Fig. 1

The Office Action must explain the pertinence of references where the correspondence is not readily discernible. "The pertinence of each reference, if not apparent, must be clearly explained." *M.P.E.P.* § 706 citing 37 C.F.R. § 1.104. The Office Action appears to suggest that because the end result of the different circuit implementations is similar (*i.e.*, both perform an affine transformation) there is

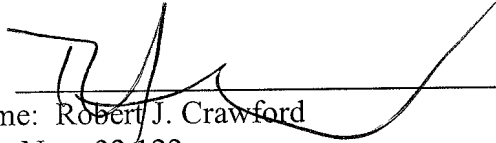
correspondence. Showing the same end result is not sufficient to show correspondence to limitations directed toward structural differences in how the result is achieved. "Even if the prior art device performs all the functions recited in the claim, the prior art cannot anticipate the claim if there is any structural difference." M.P.E.P. § 2114. Here, the prior art neither performs all the functions nor has identical structure. At best, the Office Action has only asserted correspondence to the end result of implementation of a Rijndael Block Cipher. As Applicant's claims are directed toward a specific implementation of a Rijndael Block Cipher, generic recitation of the end results of different implementations is insufficient to show correspondence.

In view of the remarks above, Applicant believes that each of the rejections has been overcome and the application is in condition for allowance. Should there be any remaining issues that could be readily addressed over the telephone, the Examiner is asked to contact the agent overseeing the application file, David Cordeiro, of NXP Corporation at (408) 474-9063 (or the undersigned).

Please direct all correspondence to:

Corporate Patent Counsel
NXP Intellectual Property & Standards
1109 McKay Drive; Mail Stop SJ41
San Jose, CA 95131

CUSTOMER NO. 65913

By: 
Name: Robert J. Crawford
Reg. No.: 32,122
Shane O. Sondreal
Reg. No. 60,145
651-686-6633
(NXPS.604PA)